PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-184992
(43)Date of publication of application : 09.07.1999

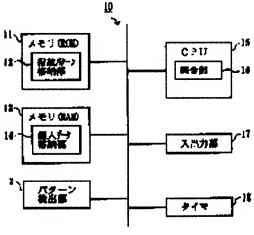
(51)Int.Cl. G06K 17/00
G06T 7/00
G06K 19/10
G06K 19/07

(21)Application number : 09-354268
(22)Date of filing : 24.12.1997

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : YAMAKITA TORU

(54) IC CARD AND DEVICE FOR INSERTING THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To attain improvement in security by judging whether an IC card is used by an authorized user or not while using a fingerprint pattern.
SOLUTION: A memory 11 is provided with a fingerprint pattern storage part 12 as a ROM area for storing the fingerprint pattern of a prescribed finger of the card user. A pattern detecting part 2 detects the rugged surface of an object pressed onto its surface. A collation part 16 of a CPU 15 is provided by executing one part of a program and collates the fingerprint pattern stored in the fingerprint pattern storage part 12 with the fingerprint pattern of the card user read by the pattern detecting part 2. Thus, the IC card itself judges whether a person to use the IC card is the authorized user or not and reports the judged result to a main body device. When the IC card is used by a person, who is not an authorized user (illegally used), the main body device inhibits processing based on that IC card.



LEGAL STATUS

[Date of request for examination] 09.12.2002
[Date of sending the examiner's decision of rejection] 31.05.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－184992

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｖ
			Ｂ
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｓ
19/07			Ｊ

審査請求　未請求　請求項の数７　ＯＬ　（全 15 頁）

(21)出願番号　特願平9－354268

(22)出願日　平成９年(1997)12月24日

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号

(72)発明者　山北　徹
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

(74)代理人　弁理士　阪本　紀康

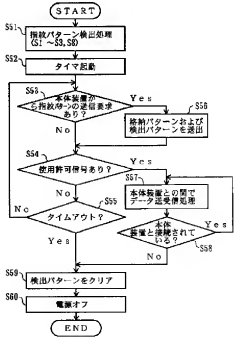
(54)【発明の名称】　ＩＣカードおよびＩＣカードが挿入される装置

(57)【要約】

【課題】　使用者の負担を小さくしながら高いセキュリティが得られるＩＣカードおよびそのＩＣカードが挿入される装置を提供する。

【解決手段】　ＩＣカードは、使用者の指紋パターンを検出し、その検出した指紋パターンおよび予め格納してある指紋パターンを本体装置に送出する。本体装置は、これら２つの指紋パターンを照合し、一致した場合にはＩＣカードに対して使用許可信号を送信する。ＩＣカードは、使用許可信号を受信すると、本体装置との間でデータの送受信を行う。

第３の実施例のＩＣカードの処理のフローチャート



【特許請求の範囲】
【請求項１】　物体の表面のパターンを検出する検出手段と、
指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有し、
上記照合手段が出力する照合結果に基づいて処理を許可するか否かを判断する装置に挿入されるＩＣカード。
【請求項２】　上記照合手段は、上記照合結果を所定期間出力する請求項１に記載のＩＣカード。
【請求項３】　物体の表面のパターンを検出する検出手段と、
指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段と、を有し、
上記出力手段が出力する各指紋パターンを照合して処理を許可するか否かを判断する装置に挿入されるＩＣカード。
【請求項４】　ＩＣカードが挿入される装置であって、
上記ＩＣカードに予め格納されている指紋パターンとそのＩＣカードが検出した指紋パターンとの照合結果として、それら２つの指紋パターンが互いに一致している旨の通知をそのＩＣカードから受信した際に、そのＩＣカードに基づく処理を許可する装置。
【請求項５】　上記ＩＣカードが、照合結果として、上記２つの指紋パターン間の類似度を複数段階で評価した結果を出力した場合、
類似度の段階に応じて、
そのＩＣカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのＩＣカードに基づく処理を許可し、
もしくは、そのＩＣカードに基づく処理を禁止する、
請求項４に記載の装置。
【請求項６】　ＩＣカードが挿入される装置であって、
上記ＩＣカードに予め格納されている指紋パターンおよびそのＩＣカードが検出した指紋パターンをそのＩＣカードから受信する受信手段と、
上記２つの指紋パターンを照合し、それらが互いに一致していた場合にそのＩＣカードに基づく処理を許可する照合手段と、
を有する装置。
【請求項７】　上記照合手段は、上記２つの指紋パターン間の類似度を複数段階で評価し、類似度の段階に応じて、
そのＩＣカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのＩＣカードに基づく処理を許可し、
もしくは、そのＩＣカードに基づく処理を禁止する、
請求項６に記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード、および挿入されたＩＣカードとの間でデータを送信または受信する装置に係わる。
【０００２】
【従来の技術】従来から、使用する者の身分証明（ＩＤ）としての機能が電子的に組み込まれたカードが広く普及している。たとえば、銀行等の口座にアクセスするための、いわゆるキャッシュカードやクレジットカード、あるいはドアのロックを解除したり、各種装置を起動するためのＩＤカードなどである。これらのカードには、通常、そのカードの使用者を識別する情報が書き込まれた磁気フィルム等が貼り付けられている。そして、使用時には、そのカードが挿入された装置がその識別情報を読み取り、アクセス等の処理を許可するか否かなどを判断する。
【０００３】ところが、上述のような単純な方式だと、カードを紛失した場合などには、それを拾った他人が不正にそのカードを使用できることになる。そこで、キャッシュカード等においては、上述のような磁気フィルム等に書き込まれた識別情報と共に、暗証番号（パスワード）が併用されることが一般的である。例えば、キャッシュカードが挿入されると、ユーザに暗証番号を要求し、その要求に対して予め登録されている正規の暗証番号が投入されたときにのみアクセスを許可するようなシステムは広く実施されている。
【０００４】また、近年、上述のようなカードにインテリジェントな機能を持たせるために集積回路を組み込んだカード型の機器（通常、ＩＣカードと呼ばれることが多いので、以下、そのように呼ぶことにする）の研究・開発が盛んである。ＩＣカードは、将来、電子マネーや電子財布の分野においてその中心的な役割を担うことが予想されているので、特に、他人の不正使用を防ぐために高いセキュリティを確保することが必須の要件となっている。
【０００５】
【発明が解決しようとする課題】現在、他人による各種カード類（ＩＣカードを含む）の不正使用を防ぐ手法としては、暗証番号（パスワード）が最も一般的である。ところが、この場合、各カード使用者は、暗証番号を覚えておく必要があり、特に所持するカードの枚数が多いとその負担が大きくなっていた。また、暗証番号は、流出してしまう恐れがあった。
【０００６】本発明の課題は、上述の問題を解決することであり、使用者の負担を小さくしながら高いセキュリティが得られるＩＣカードおよびそのＩＣカードが挿入

される装置を提供することである。

【０００７】

【課題を解決するための手段】本発明のＩＣカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有する。

【０００８】上記ＩＣカードが挿入される装置は、そのＩＣカードに予め格納されている指紋パターンとそのＩＣカードが検出した指紋パターンとの照合結果としてそれら２つの指紋パターンが互いに一致している旨の通知をそのＩＣカードから受信した際に、そのＩＣカードに基づく処理を許可する構成である。

【０００９】上記構成によれば、格納手段に格納されている指紋パターンを持つ者以外の者がこのＩＣカードを使用すると、照合手段による照合結果は不一致となる。したがって、上記ＩＣカードが挿入される装置は、そのＩＣカードに基づく処理を禁止する。このようにして、指紋パターンにより不正使用を防ぐ。

【００１０】本発明の他の形態のＩＣカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段とを有する。

【００１１】上記他の形態のＩＣカードが挿入される装置は、そのＩＣカードに予め格納されている指紋パターンおよびそのＩＣカードが検出した指紋パターンをそのＩＣカードから受信する受信手段と、上記２つの指紋パターンを照合し、それらが互いに一致していた場合にそのＩＣカードに基づく処理を許可する照合手段と、を有する構成である。この形態の作用は、上述した作用と同じである。

【００１２】

【発明の実施の形態】以下、本発明の実施形態について図面を参照しながら説明する。図１(a) および(b) は、本実施形態のＩＣカードの外観図である。ＩＣカード１は、たとえば、銀行口座へのアクセス、商品購入時の支払い、ドアロックの解除、あるいは各種装置の起動などに際して使用されるカード型の機器である。ＩＣカード１は、その表面の一部に、パターン検出部２が設けられている。パターン検出部２は、そこに接触された物体の表面のパターン（凹凸パターン等）を検出する機能を有し、本実施形態では、カード使用者の指紋パターンを読み取るために使用される。

【００１３】カード使用者は、ＩＣカード１を使用する際には、まず、スイッチをオンにした後、予め決めてある所定の指をパターン検出部２に押圧する。図１(a) に示す例では、右手の人差し指をパターン検出部２に押圧する例を示している。所定の指をパターン検出部２に押圧するときには、指紋パターンが確実に検出されるように、親指を使ってＩＣカード１を挟み付けるようにすることが望ましい（図１(b) 参照）。

【００１４】ＩＣカード１には、その使用者の所定の指（図１に示す実施例では、右手の人差し指）の指紋パターンが予め格納されている。そして、後述する第１および第２の実施例では、ＩＣカード１は、その予め格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合し、その照合結果を出力する。また、第３の実施例では、ＩＣカード１は、そのカードが挿入される本体装置に対して、上記予め格納されている指紋パターンおよびパターン検出部２により検出された指紋パターンを出力し、その本体装置がそれらの指紋パターンを照合する。そして、本体装置は、各実施例において、上記２つの指紋パターンが一致したときに、ＩＣカード１に基づく処理（ＩＣカード１を用いたアクセスを含む）を許可し、以降、その間でデータを送受信する。

第１の実施例

第１の実施例は、ＩＣカードに指紋照合機能を持たせた構成である。

【００１５】図２は、第１（および第２）の実施例のＩＣカード１０の構成図である。メモリ１１は、ＲＯＭ領域であり、カード使用者の所定の指の指紋パターンを格納するための指紋パターン格納部１２を含む。この指紋パターンは、たとえば、カードの発行時に格納される。メモリ１１には、後述するフローチャートの処理を記述したプログラム等も格納されている。メモリ１３は、ＲＡＭ領域であり、上記プログラムを実行する際に使用される領域の他、カード使用者の個人情報を格納する個人データ格納部１４が設けられている。個人データ格納部１４は、たとえば、このＩＣカード１０が電子マネーシステムにおける電子財布であったとすると、「財布の中の金額」に相当する情報などを格納する。なお、個人データ格納部１４は、不揮発性メモリ領域に設けられる。

【００１６】パターン検出部２は、その表面に押圧された物体の表面の凹凸を検出する装置であり、微細化技術の進歩によりＩＣカードに組み込むことができる程度に薄く形成されている。パターン検出部２は、たとえば、光源および２次元フォトセンサを含み、その２次元フォトセンサを構成する多数の受光素子がそれぞれ検出する受光レベルに対応する電流値または電圧値をシリアル形式またはパラレル形式で出力する。なお、本発明の出願人は、先に、十分に薄型でありながら高い精度で物体の表面の凹凸パターンを検出することができる読取装置について特許出願をしている（特願平９－２２２０１８号）。

【００１７】ＣＰＵ１５は、メモリ１１に格納されているプログラムを実行する。ＣＰＵ１５は、照合部１６を備える。照合部１６は、上記プログラムの一部を実行す

ることにより実現され、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により読み取られたカード使用者の指紋パターンとを照合する。入出力部１７は、このＩＣカード１０が挿入される本体装置との間でデータを送受信する。タイマ１８は、ＣＰＵ１５により起動され、所定時間が経過するとＣＰＵ１５に割込信号を送出する。

【００１８】図３は、第１（および第２）の実施例の本体装置２０の構成図である。この本体装置２０には、図２に示したＩＣカード１０が挿入される。ＩＣカード１０は、カード挿入部２１に挿入される。カード挿入部２１は、ＩＣカード１０とのインタフェースをとるためのＩ／Ｆ部２２を備える。ＣＰＵ２３は、メモリ２４に格納されているプログラムを実行することにより、ＩＣカード１０とのデータの授受、また、必要に応じて不図示の外部装置（ホストコンピュータなど）とのデータの授受を制御する。メモリ２４は、後述するフローチャートの処理を始め、この本体装置２０の各ソフトウェア処理を記述したプログラムおよびこの本体装置２０が使用する各種データを格納する。なお、ここでは、カード挿入部２１、ＣＰＵ２３およびメモリ２４が１つの装置の中に設けられているように記載しているが、これらを互いに異なる場所に設け、通信回線等を用いた互いに接続する構成であってもよい。

【００１９】図４および図５は、第１の実施例におけるＩＣカードの処理のフローチャートである。この処理は、ＩＣカードの電源をオンにしたことをトリガとして実行される。

【００２０】ステップＳ１では、電源がオンにされたときから一定時間内にパターン検出部２に入力があったか否かを調べる。この処理は、たとえば、パターン検出部２の出力が変化したか否かを調べるものである。パターン検出部２に入力があった場合には、ユーザが所望の指の指先（指紋が形成されている部分）をパターン検出部５に押圧したものと見なし、ステップＳ２へ進み、一方、入力が無かった場合には、ステップＳ８においてＩＣカードの電源をオフにする。

【００２１】ステップＳ２では、指紋パターンを検出する。すなわち、パターン検出部２の出力を取り込む。この指紋パターンは、たとえば、メモリ１３の所定の領域に保持される。ステップＳ３では、指紋パターンを適切に検出できたか否かを判断する。すなわち、ユーザの指がパターン検出部２に一定時間以上固定されなかった場合や、押圧が弱く接触面積が小さかった場合などには、指紋パターンを再生できないので、このステップで指紋パターンを適切に検出できたか否かを判断している。指紋パターンを適切に検出できた場合には、ステップＳ４へ進み、検出できなかった場合にはステップＳ１へ戻る。

【００２２】ステップＳ４では、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合する。この処理は、例えば、上記２つの指紋パターンの類似度を数値化する手順を含む。

【００２３】ステップＳ５では、上記ステップＳ４により得られた類似度を表す値が、予め設定してある閾値を越えるか否かに従って「一致／不一致」を判断する。上記２つの指紋パターンが互いに一致していた場合には、ステップＳ６において、ＯＫ信号を出力する。この処理は、例えば、このＩＣカードが挿入される本体装置２０のＩ／Ｆ部２２と接触する端子の中の所定の１つを「Ｌ」レベルから「Ｈ」レベルに切り換えるものである。ステップＳ７では、タイマ１８を起動する。

【００２４】ステップＳ１１およびＳ１２では、使用許可信号を受信しているか否かを調べる。なお、この使用許可信号は、後述説明するが、図４に示した本体装置２０により生成される信号であり、本体装置２０がそこに挿入されたＩＣカードに基づく処理を許可すると判断した際に本体装置２０によって出力される。ここで、タイマ１８に設定されている所定の時間が経過する前に使用許可信号を受信した場合には、ステップＳ１６およびＳ１７において、本体装置２０との間でデータを送受信する処理を実行する。この処理は、ＩＣカードが本体装置２０と接続されている間は継続される。

【００２５】本体装置２０がこのＩＣカードを排出するなどして本体装置２０との接続が終了すると、ステップＳ１３へ進んでＯＫ信号をリセットする。すなわち、ＯＫ信号の送出を停止する。続いて、ステップＳ１４では、ステップＳ２においてパターン検出部２により検出した指紋パターンをクリアする。そして、ステップＳ１５において、このＩＣカードの電源をオフにする。

【００２６】一方、ステップＳ１１およびＳ１２において、タイマ１８に設定されている所定の時間が経過するまでに使用許可信号を受信できなかった場合、すなわち、タイマ１８がタイムアウトした場合には、ステップＳ１６およびＳ１７を実行することなくステップＳ１３へ進む。すなわち、本体装置２０から使用許可信号を受信できなかった場合には、このＩＣカードは、本体装置２０との間でデータを授受できない。

【００２７】なお、ステップＳ５において、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとが一致しないと判断した場合には、ＯＫ信号を出力することなくステップＳ１４へジャンプし、その検出した指紋パターンをクリアした後に電源をオフにする。

【００２８】図６は、第１の実施例における本体装置の処理のフローチャートである。この処理は、ＩＣカード１０が挿入されたことをトリガとして実行される。ステップＳ２１およびＳ２２では、ＩＣカード１０が挿入されたときから一定時間内にそのＩＣカード１０からＯＫ

信号を受信したか否かを調べる。ＯＫ信号は、上述したように、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとが一致した場合にＩＣカード１０により出力される信号である。ＯＫ信号を受信した場合には、ステップＳ２３へ進み、一方、受信できなかった場合には、ステップＳ２５において挿入されたＩＣカード１０を排出する。

【００２９】ステップＳ２３では、ＩＣカード１０へ使用許可信号を送出する。この使用許可信号は、図５のステップＳ１１およびＳ１２において監視される信号であり、ＩＣカード１０は、この信号を受信すると、この本体装置とデータを授受できる状態になる。ステップＳ２４では、ＩＣカード１０との間でデータを送受信する処理を実行する。なお、上述したＯＫ信号は、ＩＣカードの正規の使用者（所有者）とそのＩＣカードに指紋を読み取らせた者とが一致しているか否かを表す情報なので、そのＩＣカードの使用者を識別する情報はこのステップＳ２４において受信する。したがって、もし、そのＩＣカードの使用者を識別する情報が正規に登録されていなかった場合などには、ＯＫ信号を受信した場合であってもそのＩＣカードに基づく処理を拒絶することがある。また、この本体装置が、ＩＣカード１０とのデータの授受に際して不図示のホストコンピュータなどとの間でデータを授受する必要がある場合には、その処理はステップＳ２４と並列に実行される。

【００３０】このように、第１の実施例では、ＩＣカードを使用する者が正規の使用者であるか否かをＩＣカード自身が判断し、その判断結果を本体装置に通知する。そして、本体装置は、正規の使用者でない者の使用（すなわち、不正使用）であった場合には、そのＩＣカードに基づく処理を禁止する。

第２の実施例

第２の実施例は、第１の実施例の構成に加え、指紋パターンの一致／不一致の判断が微妙な時に、使用者にパスワードを要求する機能を設けた構成である。なお、第２の実施例におけるＩＣカードおよび本体装置の構成は、第１の実施例と同じであり、それぞれ図２および図３に示した通りである。

【００３１】近年では、画像認識技術が進歩してきてはいるが、一般に、パターンマッチング処理の精度は１００パーセントではない。そして、この精度は、プロセッサの能力が低い場合や、短時間で処理しなければならない状況においては、低下するものと予想される。したがって、カードを使用する者が正規の使用者であるか否かの判断は、第１の実施例において述べたように、指紋パターンの類似度を数値化してその値が所定の閾値よりも大きいか否かに基づいて決定する方式が現実的である。ところが、この閾値の設定は難しく、一致／不一致の判断を甘くすれば不正使用を排除できない恐れがあり、反対に、その判断を厳密にすれば、正規の使用者が使用しているにも係わらずその正規の使用者によるアクセスを拒絶してしまうことも起こりかねない。

【００３２】そこで、第２の実施例では、ＩＣカードは、指紋パターンの類似度を複数段階で評価し、ＩＣカードに基づく処理を許可するか否かに際して、きめ細かい判断をできるようにした。具体的には、指紋パターンの類似度を、「非常に高い」、「比較的高い」および「低い」の３段階で評価して出力し、本体装置は、「類似度が非常に高い」を受信したときには、そのまま処理を許可するが、「類似度が比較的高い」を受信したときには、使用者にパスワードを要求する。

【００３３】図７は、第２の実施例におけるＩＣカードの処理のフローチャートである。この処理は、第１の実施例と同様に、ＩＣカードの電源をオンにしたことをトリガとして実行される。なお、図７において、照合処理（ステップＳ７）、タイマ起動処理（ステップＳ７）、クリア処理（ステップＳ１４）、電源オフ処理（ステップＳ１５）は、第１の実施例と同じである。

【００３４】ステップＳ３１では、パターン検出部２により指紋パターンを検出する。この処理は、第１の実施例のステップＳ１～Ｓ３およびＳ８と同じである。続いて、ステップＳ４において、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合し、その類似度を数値化する。

【００３５】ステップＳ３２では、ステップＳ４で得られた類似度が、「非常に高い」に属するか否かを調べる。類似度が非常に高ければ、ステップＳ３３においてＯＫ１信号を出力し、そうでなければ、ステップＳ３４へ進む。ステップＳ３４では、ステップＳ４で得られた類似度が、「比較的高い」に属するか否かを調べる。類似度が比較的高ければ、ステップＳ３５においてＯＫ２信号を出力する。ＯＫ１信号またはＯＫ２信号を出力した場合には、ステップＳ７において、タイマ１８を起動する。

【００３６】ステップＳ３６は、使用許可信号を監視する処理、および使用許可信号を受信した場合に本体装置との間でデータを送受信する処理である。これらの処理は、第１の実施例のステップＳ１１、Ｓ１２、Ｓ１６およびＳ１７と同じである。ステップＳ３７では、ＯＫ１信号またはＯＫ２信号をリセットする。即ち、ＯＫ１信号またはＯＫ２信号の出力を停止する。なお、これらの信号をリセットする処理は、タイマ１８のタイムアウトした場合、あるいは本体装置から使用許可信号を受信した場合に実行される。この後、ステップＳ１４およびＳ１５において、パターン検出部２により検出したパターンをクリアし、ＩＣカードの電源をオフにする。

【００３７】なお、ステップＳ４で得られた類似度が低いと判断した場合（ステップＳ３２：Ｎｏ、且つステッ

プＳ３４：Ｎｏ）には、正規の使用者でない者がこのＩＣカードを使用しているものとみなし、ＯＫ１信号またはＯＫ２信号のいずれも出力することなく、ステップＳ１４へジャンプする。

【００３８】図８は、第２の実施例における本体装置の処理のフローチャートである。この処理は、第１の実施例と同様に、ＩＣカードが挿入されたことをトリガとして実行される。

【００３９】ステップＳ４１～Ｓ４３は、挿入されたＩＣカードから所定時間内にＯＫ１信号またはＯＫ２信号を受信したか否かを監視する処理である。ＯＫ１信号を受信した場合、すなわちＩＣカードにおいて照合された２つの指紋パターンの類似度が非常に高い旨の通知を受けた場合には、そのＩＣカードを使用している者が正規の使用者であるとみなし、ステップＳ２３において使用許可信号を送出する。そして、ステップＳ２４において、ＩＣカードとの間でデータを送受信する処理を実行する。これらのステップＳ２３およびＳ２４は、第１の実施例における処理と同じである。

【００４０】ＯＫ信号２を受信した場合、すなわちＩＣカードにおいて照合された２つの指紋パターンの類似度が比較的高い旨の通知を受けた場合には、そのＩＣカードを使用している者が正規の使用者である可能性が高いもののそうでない可能性もあるとみなし、ステップＳ４４においてパスワードを要求する。続いて、ステップＳ４５では、まず、その挿入されたＩＣカードを識別する情報をそのＩＣカードから読み取り、その識別情報に対して予め登録されているパスワードを抽出しておく。そして、上記要求に応答してカード使用者により入力されたパスワードとその予め登録されているパスワードとを照合する。ステップＳ４６では、ステップＳ４５における照合の結果を判断し、パスワードが一致していればステップＳ２３へ進んで、使用許可信号を送出する処理、およびＩＣカードとの間でデータを送受信する処理を実行し、一致していなければ、これらの処理をスキップしてステップＳ２５へ進む。

【００４１】所定時間内にＯＫ１信号またはＯＫ２信号のいずれも受信できなかった場合には、ＩＣカードを使用している者が正規の使用者ではないとみなし、使用許可信号を送出することなくそのＩＣカードを排出する。

【００４２】このように、第２の実施例では、指紋パターンの照合結果のみではＩＣカードを使用している者が正規の使用者であるのか否かを判断できない場合に、使用者にパスワードを入力させる構成を導入した。この結果、正しいパスワードを知らない不正使用者を確実に排除できると共に、正規の使用者が使用できないような状況は回避される。また、パスワードを併用するので、指紋パターンの照合の精度がさほど高くなくてもＩＣカードを使用する者が正規の使用者であるか否かを判断できる。したがって、ＩＣカード内に設けるＣＰＵの性能はさほど高くなくてもよく、ＩＣカードの自体のコストアップを抑えられる。

第３の実施例

第３実施例は、指紋パターンを照合する処理をＩＣカードが挿入される本体装置において実行する構成である。

【００４３】図９は、第３の実施例のＩＣカードの構成図である。第３の実施例のＩＣカードは、基本的には第１または第２の実施例と同じ構成であるが、指紋パターンを照合する処理を実行しないので、照合部１６は設けられていない。

【００４４】図１０は、第３の実施例の本体装置の構成図である。第３の実施例の本体装置は、基本的には第１または第２の実施例と同じ構成であるが、指紋パターンを照合する処理を実行する。このため、ＣＰＵ３１がメモリ２４に格納されているプログラムを実行することによって得られる機能の一部として照合部３１が設けられている。

【００４５】図１１は、第３の実施例におけるＩＣカードの処理のフローチャートである。この処理は、第１または第２の実施例と同様に、ＩＣカードの電源をオンにしたことをトリガとして実行される。

【００４６】ステップＳ５１では、パターン検出部２により指紋パターンを検出する。この処理は、第１の実施例のステップＳ１～Ｓ３およびＳ８と同じである。続いて、ステップＳ５２では、タイマ１８を起動する。

【００４７】ステップＳ５３～５５は、タイマ１８がタイムアウトする前に、このＩＣカードが挿入された本体装置から指紋パターンの送信要求を受信したか否か、および使用許可信号を受信したか否かを調べる処理である。本体装置から指紋パターンの送信要求を受信した場合には、ステップＳ５３～Ｓ５５において、指紋パターン格納部１２に格納されている指紋パターンおよびパターン検出部２により検出した指紋パターンを本体装置へ送出する。また、使用許可信号を受信した場合には、ステップＳ５７およびＳ５８において、本体装置との間でデータを送受信する処理を実行する。この処理は、このＩＣカードが本体装置と接続されている間は継続される。

【００４８】本体装置から使用許可信号を受信することなくタイマ１８がタイムアウトした場合、または本体装置との接続が終了した場合には、パターン検出部２により検出した検出パターンをステップＳ５９においてクリアし、ステップＳ６０においてこのＩＣカードの電源をオフにする。

【００４９】このように、第３の実施例のＩＣカードは、本体装置からの要求に応じて予め格納してある指紋パターンおよび検出した指紋パターンを送出する。本体装置はそれらの指紋パターンに基づいて使用を許可するか否かを判断する。そして、ＩＣカードは、本体装置から使用許可が与えられたときにのみ本体装置との間でデータの送受信が可能となる。

【００５０】図１２は、第３の実施例における本体装置の処理のフローチャートである。この処理は、第１または第２の実施例と同様に、ＩＣカードが挿入されたことをトリガとして実行される。

【００５１】ステップＳ６１～Ｓ６３は、挿入されたＩＣカードに対して指紋パターンの送出を要求し、所定時間内にその要求に応じて指紋パターンを受信できるか否かを判断する処理である。ＩＣカードから指紋パターンを受信した場合にはステップＳ６４へ進み、受信できなかった場合には、ステップＳ６８においてそのＩＣカードを排出する。

【００５２】ステップＳ６４では、ＩＣカードから受信した２つの指紋パターン、即ち指紋パターン格納部１２に格納されている指紋パターンおよびパターン検出部２により検出した指紋パターンを照合する。この処理は、たとえば、図４のステップＳ４の処理と同じであり、類似度を数値化する手順を含む。ステップＳ６５は、ステップＳ６４における照合処理の結果を参照し、上記２つの指紋が一致するのか否かを判断する。一致する場合には、ステップＳ６６においてＩＣカードに対して使用許可信号を送出し、ステップＳ６７においてそのＩＣカードとの間でデータの送受信処理を実行する。一方、上記２つの指紋が互いに一致しなかった場合は、ステップＳ６６およびＳ６７をスキップしてステップＳ６８へ進んでＩＣカードを排出する。

【００５３】このように、第３の実施例の本体装置は、挿入されたＩＣカードから予め格納してある指紋パターンおよび検出した指紋パターンを受信し、それらの指紋パターンが互いに一致した場合にのみＩＣカードに使用許可を与える。

【００５４】なお、第３の実施例においても、上述の第２の実施例と同様に、指紋パターンの照合とパスワードとを併用する構成としてもよい。このように、第３の実施例では、ＩＣカードにおいて指紋パターンの照合処理を実行しないので、ＩＣカードに設けるＣＰＵは高い性能を持つ必要がない。したがって、ＩＣカードの製造コストを低く抑えることができる。

【００５５】なお、上記第１～第３の実施例では、各ＩＣカードに１人の使用者の指紋パターンを予め格納しておく構成を示したが、本発明は、この形態に限定されるものではない。たとえば、家族や特定のグループの人間がＩＣカードを共有できるようにしてもよい。この場合、ＩＣカードに予め複数人の指紋パターンを登録しておき、検出した指紋パターンとそれら複数の指紋パターンとを１つずつ照合してゆけばよい。

【００５６】

【発明の効果】ＩＣカードが正規の使用者により使用されているのか否かの判断を指紋パターンを用いて行うので、セキュリティが高い。このとき、カード使用者は、従来のようにパスワード等を覚えておく必要はなく、また、パスワード等の流出の恐れもない。さらに、ＩＣカードを使用する際の操作も簡単である。

【図面の簡単な説明】

【図１】本実施形態のＩＣカードの外観図である。

【図２】第１および第２の実施例のＩＣカードの構成図である。

【図３】第１および第２の実施例の本体装置の構成図である。

【図４】第１の実施例のＩＣカードの処理のフローチャート（その１）である。

【図５】第１の実施例のＩＣカードの処理のフローチャート（その２）である。

【図６】第１の実施例の本体装置の処理のフローチャートである。

【図７】第２の実施例のＩＣカードの処理のフローチャートである。

【図８】第２の実施例の本体装置の処理のフローチャートである。

【図９】第３の実施例のＩＣカードの構成図である。

【図１０】第３の実施例の本体装置の構成図である。

【図１１】第３の実施例のＩＣカードの処理のフローチャートである。

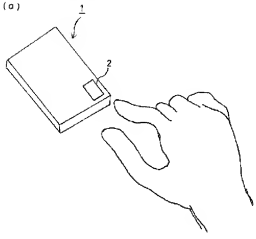
【図１２】第３の実施例の本体装置の処理のフローチャートである。

【符号の説明】

１	ＩＣカード
２	パターン検出部
１１、１３、２４	メモリ
１２	指紋パターン格納部
１５、２３	ＣＰＵ
１６、３１	照合部
１８	タイマ
２１	カード挿入部
２２	Ｉ／Ｆ部

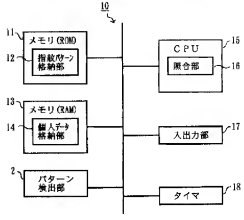
【図１】

本実施形態のＩＣカードの外観図



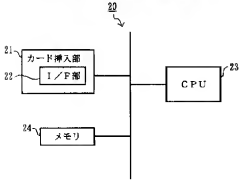
【図２】

第１および第２の実施例のＩＣカードの構成図



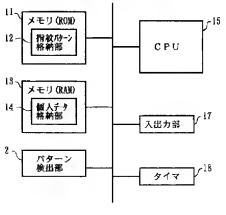
【図３】

第１および第２の実施例の本体装置の構成図



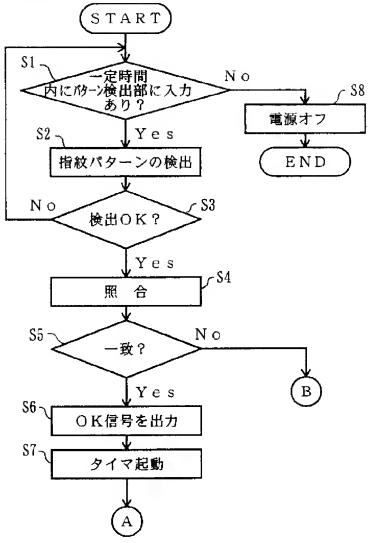
【図９】

第３の実施例のＩＣカードの構成図



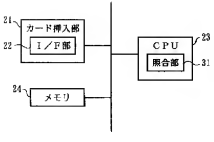
【図４】

第１の実施例のＩＣカードの処理のフローチャート（その１）



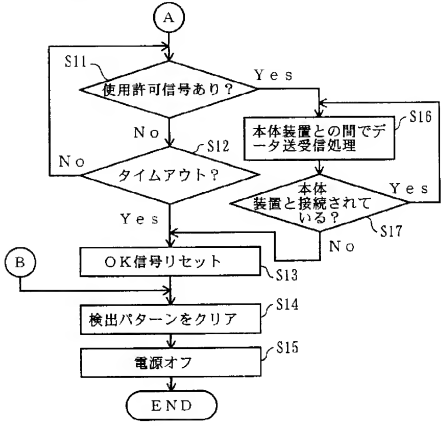
【図１０】

第３の実施例の本体装置の構成図



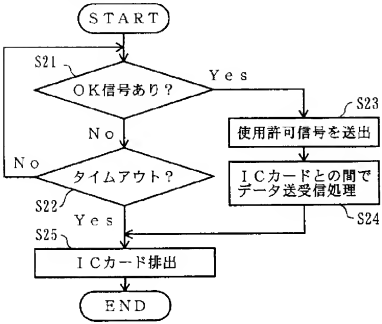
【図５】

第１の実施例のＩＣカードの処理のフローチャート（その２）



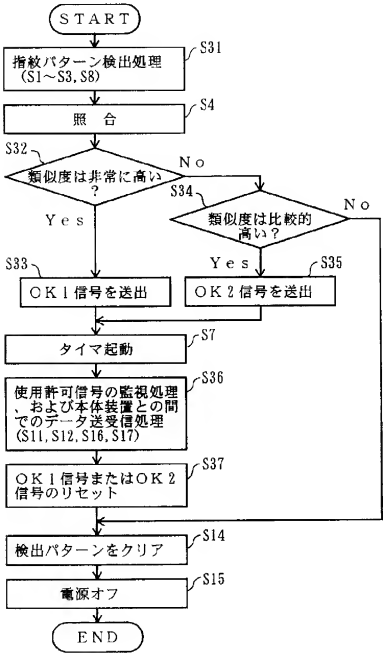
【図６】

第１の実施例の本体装置の処理のフローチャート



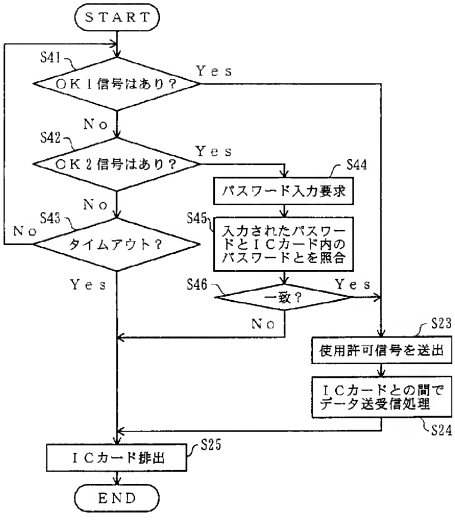
【図７】

第２の実施例のＩＣカードの処理のフローチャート



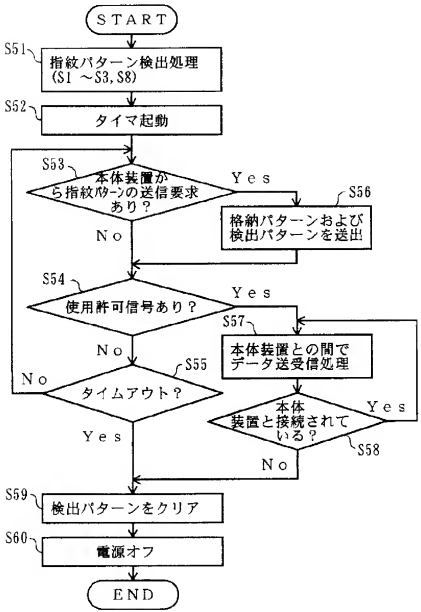
【図８】

第２の実施例の本体装置の処理のフローチャート



【図１１】

第３の実施例のＩＣカードの処理のフローチャート



【図１２】

第３の実施例の本体装置の処理のフローチャート